Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1649 12/05/14

~ Terrible Tech Annoyances ~ People Are Talking! ~ Santa Letter Scams!
~ Facebook "Threats" Case! ~ Revenge Porn Law Case! ~ Street Fighter V!
~ Airport Fraud Busts 118! ~ "Number Two" Hacker! ~ Dotcom Avoids Jail!

~ New Preview of Win 10! ~ Firefox: Yahoo Is In! ~ I Am Not A Robot!

-* Manual Account Hijacking! *-
-* FBI Warns of "Destructive" Malware! *-
-* All PayPal Accounts A Click Away from Gone *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Some would say, "Better Late Than Never!" Well, I have to apologize for this week's issue being a day late. But, I have a good excuse. As I mentioned a couple of weeks ago, we recently lost one of our canine kids. Well, we've been monitoring the web site of our local animal shelter, looking to see the comings and goings of the dogs - thinking that one just might jump out at us as a candidate for adoption. We were following one particular dog for about a week. so, yesterday, we decided to take a ride and take a look at Amy, a 7-year-old Corgi-mix. We brought Sam, our 8-year-old greyhound to see how he and Amy might get along - or him with any other dogs that might interest us if Amy didn't work out.

The two dogs hit it off fairly well. They did their sniffing and circling, and seemed okay with each other in an enclosed room. We took them out in the shelter's enclosed yard; and the two played around a bit (Sam isn't much of a dog that "plays"!). Again, they seemed okay. So, my wife and I decided that Amy would be a welcomed addition to the family; and we brought her home!

Once at home, we spent the rest of the night getting used to new surroundings and how Amy reacted to her new environment. And, we finally figured out the sleeping arrangements - Amy ended up in our bed where she settled in nicely for the night.

So, here we are, a day later. I've finally been able to put in the last bit of time getting this week's issue ready to hit the streets. Both Amy and Sam are laying down on the couch relaxing from their hectic first full day together. And, my wife and I are trying to catch up on some much-needed rest!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Leak Calls 'Street Fighter V' A PS4 and Windows Exclusive
""""""""""""""""""""""""""""""

Captain Toad: Treasure Tracker Out Now!
Happy 20th Birthday, PlayStation!
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""

Leaked Video Calls ’Street Fighter V’ A PS4 and Windows Exclusive

Earlier today Capcom’s YouTube channel accidently featured a video for Street Fighter V a bit early - it was set to be revealed either during The Game Awards later tonight or at Sony’s PlayStation Experience this weekend.

The trailer reveals some bad news for Xbox One and Wii U fans: Capcom’s popular fighting game franchise will be a Windows and PS4 exclusive. What does this mean? It means that the Xbox One and the Wii U will be missing out on one of Capcom’s most popular franchises. We’re not sure if this is a "launch exclusive" or if this means that Capcom has no plans to bring the game to any other platforms at this point.

Capcom has not officially announced Street Fighter V and the trailer for the game quickly disappeared after it made the rounds.

We will have more information on this news as it becomes available. The leaked trailer has managed to do one important thing: create buzz about Street Fighter V’s big reveal this weekend...

Captain Toad: Treasure Tracker Out Now

Nintendo has announced that Captain Toad: Treasure Tracker has launched exclusively for the Wii U console today in North America.

Captain Toad: Treasure Tracker finds players donning their head lamps to journey through more than 70 colorful levels. Each level is a self-contained puzzle full of obstacles and challenges that can only be solved by viewing the world from different angles using the Wii U GamePad controller.

The goal of every stage is to find the coveted Power Star, but Captain Toad and Toadette can also gather hidden Super Gems, 1-Up Mushrooms and shiny gold coins. Players can also complete a specific challenge on each stage that will unlock additional levels in the game.

Players that have Super Mario 3D World save data present on their Wii U systems can immediately unlock bonus content in the form of Super Mario 3D World-style stages. After completing the game, the Super Mario 3D World-style stages will also unlock for players who don t have the save data.

Captain Toad: Treasure Tracker is available in stores, at Nintendo.com and in the Nintendo eShop on Wii U for $39.99.

Report Says Console Gamers Still Prefer Physical to Digital

A new report claims that while most gamers recognize digital downloads are the future of games sales, it’s going to be a while before digital trumps physical sales on consoles.

In a study called The Democracy of Downloading: What Gamers Expect (and Want) from Digital Distribution , entertainment marketing firm MarketCast interviewed 1,000 gamers on both PC and console to determine what customers want and expect from digital products.

The study found about 85 percent of gamers interviewed agreed that the transition to digital would make games more democratic by giving them a better chance to vote with their wallets, and level the playing field for smaller studios.

Just under 20% of console game purchases were digital, according to MarketCast. However, people buying digital console games did so in addition to the standard number of physical game purchases. This jibes with the quarterly reports of major publishers like Activision and EA, who get most of their growing digital revenues from DLC and subscription services rather than full game sales.

100 PC gamers, all users of the Steam distribution platform, were interviewed to provide contrast to the experience of Xbox Live and PlayStation Network users. Steam’s PC audience reported higher satisfaction with their digital experience than console gamers.

The study shows console gamers like the convenience of digital downloads, but are concerned with what happens after purchase, and miss the feeling of ownership that comes with an actual disc. While a physical game can be resold if a user doesn’t like it, that’s not so easy at the moment if the game is digital and activated by a product key.

So what will trigger the digital revolution on consoles? The MarketCast report argues that it won’t come until streaming services as reliable as Netflix are available to gamers, digital retailers begin offering easy-to-use resale options for unwanted old games, or the cost of digital games are lowered to below $60.
Those interviewed were twice as likely to want a streaming service for games on an all digital console in the future, though they admitted the technology might not be ready quite yet.

With that in mind, services like PlayStation Now, OnLive, and Nvidia Grid look pretty timely even if they are in their infancy. IGN took a look at Nvidia’s Grid streaming service and found that it was already twice as fast as PlayStation Now.

Happy 20th Birthday, PlayStation!

On Dec. 3, 1994, electronics giant Sony released an unassuming gray box that could play CD-based video games. And while the PlayStation brand would go on to bigger, better things, the company owes a debt to the

system that got it started.

The PlayStation was a revolutionary. It set standards the industry would follow for decades. Crucially, it kicked off a legacy that turned Sony into a household video game name.

But it wasn t always a feather in the company s cap. While the PlayStation division is currently one of the pillars Sony is relying on to help turn around its struggling empire, the company wasn t thrilled to get into the gaming business. In fact, were it not for longtime rival Nintendo, Sony may be, at best, a sideline player in today s gaming scene.

It all started in 1988, when Nintendo and Sony agreed to work together on a CD-ROM device for the Super Nintendo system. Three years later, Sony debuted the machine at the Consumer Electronics Show.

But the day after the reveal, Nintendo dropped a bombshell, declaring it would not work with Sony and would instead partner with Philips, an announcement that made Sony officials flip their lids. Sony President Norio Ohga quickly assigned Ken Kutaragi (who has since been dubbed The Father of the PlayStation) to the task of developing a competitive system.

Typically, major business decisions made in the heat of anger tend to flop. As Sony officials calmed down a bit, they began to reconsider the directive. In May 1992, Kutaragi was forced to defend his project to company officials, who were skeptical about diving headfirst into a video game industry dominated by Nintendo and Sega. Kutaragi was successful, and the PlayStation division was shifted from the main corporate umbrella to Sony Music, where it found a more welcoming environment.

Game companies, fortunately, were a little easier to convince. Developers quickly fell in love with the system s CD-ROM storage system and 3D graphics and signed on to make games.

When the system hit store shelves 20 years ago in Japan (it wouldn t launch in North America for nine more months), gamers liked that the $300 system was $100 cheaper than the competing Sega Saturn. The first 100,000 units immediately sold out, and it didn t slow down. By the time production on the original PlayStation ended in 2006, the system had sold 100 million units, a home console record at the time (it would eventually be eclipsed by the PlayStation 2).

The secret of that success? The CD format, for one thing, which was cheaper than the N64 s chunky cartridges. But where Sony truly left Nintendo behind was in its willingness to let third-party game makers experiment and create the bulk of the software for the system.

Over the course of its life, nearly 8,000 games were made for the PlayStation, with only a handful coming from Sony s internal studios. Third-party blockbusters like Resident Evil, Final Fantasy VII, Metal Gear Solid, Tekken, and Tony Hawk s Pro Skater all got their console start on the PlayStation. Despite initially releasing simultaneously on the PlayStation and Saturn, Tomb Raider and its immediate sequels called Sony s machine home. Add Sony-created hits like Gran Turismo, Crash Bandicoot, Spyro the Dragon, and the cult fave PaRappa the Rapper, and the system simply outplayed the competition.

Sony Computer Entertainment, founded by my mentor Ken Kutaragi, was a

project borne out of sincere passion and deep admiration for the craft of game development, said Shuhei Yoshida, president of Sony Computer Entertainment Worldwide Studios in a blog post. The mid 90s were an exciting time for game developers, driven by the explosion of powerful but affordable 3D graphics rendering hardware and the birth of many young and adventurous development studios. The original PlayStation was meant to embody that sense of adventure and discovery, that sense that anything was possible.

 We sincerely thank you for joining us on our exciting 20-year journey. You have made every bump and scrape we took along the way worthwhile.

Sony is still a leader in the video game world. The PS4 is currently the best-selling console of this generation and is serving as the launching pad for several new initiatives, including a game streaming service (PlayStation Now) and an over-the-top television network (Vue).

But the original PlayStation, whose blocky graphics wowed us in the 90s, will always hold a warm spot in gamers hearts. For a system that almost didn t make it out of the gate, the PlayStation built a legacy few companies can match.

To celebrate the milestone, Sony has announced a limited-edition, retro-looking PlayStation 4 that features the gray color of the original system. It also happens to coincide with the company s open-to-the-public PlayStation Experience event in Las Vegas.

Atari: The Potential of 35-60 Year Olds, And Why Children Are "Impossible"

Atari CEO Frederic Chesnais has warned game developers that their products now need to compete against messaging apps, not just other forms of entertainment.

"We are not just fighting against the other publishers, the way I see it is we are fighting for the allocation of time and money," he said as part of his Game Monetization USA talk on the next generation of gamers.

"[Time] is only 24/7, maybe with multi-tasking it’s 48/7 because we can do two things at the same time, but for me it’s really a question of fighting for the the allocation of time. If you spend time on Snapchat you’re not spending time on my game."

He also said that developers shouldn’t just think of the next generation of gamers as young people, but as audiences that haven’t yet been served by traditional games.

"I personally believe that today in our industry there’s a kind of black hole between 35 and 60 years old," he said.

"People have money, they have time, they just don’t necessarily play Call Of Duty or Fallout or these big games where you have to spend three or four hours."

He admitted that Atari still wasn’t sure exactly which games would be most successful with this untapped audience; Atari has launched social casino titles, and Chesnais mentioned Clash Of Clans.

"It may be less glamorous for us to target that generation because everyone wants to be the next guy who is going to invent Call Of Duty but money wise, in terms of investment and trying to create a big entertainment property I think that there's an opportunity here."

In fact, as well as rooting for this older generation of gamers Chesnais was quick to dismiss children as a potential revenue stream, calling it impossible.

"They have no credit card, they are not online; if they are using their parent's iPhone to make the micro-transactions you know that you're going to get a complaint."

He also urged developers to cancel mobile games that were not working before they were released, rather than pushing forward and investing more and more in QA and marketing costs. He pointed to RollerCoaster Tycoon 4 Mobile which Atari released in April. Today it has 10 million downloads and is making money, but Chesnais said that the company had made some mistakes with the initial release and the game needed six or seven updates and half the features changed.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

More Atari Games From Landfill Up For Auction

Another batch of Atari game cartridges unearthed in a New Mexico landfill are going up for auction.

Between 300 and 400 games uncovered in an Alamogordo dump in April are now open for bidding on eBay.

Joe Lewandowski, a consultant for the film companies that documented the dig, says the offerings include "Yars' Revenge," ''Super Breakout" and "E.T. The Extra-Terrestrial."

Lewandowski says 50 games at a time will be posted on eBay over the next couple of weeks.

He says there's no telling how much money the games will bring in. He says he is still surprised an auction earlier this month generated $37,000.

Lewandowski plans to present a report on the eBay auction's progress to Alamogordo commissioners Tuesday.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

FBI Warns of 'Destructive' Malware in Wake of Sony Attack

The Federal Bureau of Investigation warned U.S. businesses that hackers have used malicious software to launch a destructive cyberattack in the United States, following a devastating breach last week at Sony Pictures Entertainment.

Cybersecurity experts said the malicious software described in the alert appeared to describe the one that affected Sony, which would mark first major destructive cyber attack waged against a company on U.S. soil. Such attacks have been launched in Asia and the Middle East, but none have been reported in the United States. The FBI report did not say how many companies had been victims of destructive attacks.

"I believe the coordinated cyberattack with destructive payloads against a corporation in the U.S. represents a watershed event," said Tom Kellermann, chief cybersecurity officer with security software maker Trend Micro Inc. "Geopolitics now serve as harbingers for destructive cyberattacks."

The five-page, confidential "flash" FBI warning issued to businesses late on Monday provided some technical details about the malicious software used in the attack. It provided advice on how to respond to the malware and asked businesses to contact the FBI if they identified similar malware.

The report said the malware overrides all data on hard drives of computers, including the master boot record, which prevents them from booting up.

"The overwriting of the data files will make it extremely difficult and costly, if not impossible, to recover the data using standard forensic methods," the report said.

The document was sent to security staff at some U.S. companies in an email that asked them not to share the information.

The FBI released the document in the wake of last Monday's unprecedented attack on Sony Pictures Entertainment, which brought corporate email down for a week and crippled other systems as the company prepares to release several highly anticipated films during the crucial holiday film season.

A Sony spokeswoman said the company had restored a number of important services and was working closely with law enforcement officials to investigate the matter.

She declined to comment on the FBI warning.

The FBI said it is investigating the attack with help from the Department of Homeland Security. Sony has hired FireEye Inc's Mandiant incident response team to help clean up after the attack, a move that experts say indicates the severity of the breach.

While the FBI report did not name the victim of the destructive attack in its bulletin, two cybersecurity experts who reviewed the document said it was clearly referring to the breach at the California-based unit of Sony Corp.

"This correlates with information about that many of us in the security industry have been tracking," said one of the people who reviewed the document. "It looks exactly like information from the Sony attack."

FBI spokesman Joshua Campbell declined comment when asked if the software had been used against the California-based unit of Sony Corp, although he confirmed that the agency had issued the confidential "flash" warning, which Reuters independently obtained.

"The FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations," he said. "This data is provided in order to help systems administrators guard against the actions of persistent cyber criminals."

The FBI typically does not identify victims of attacks in those reports. Hackers used malware similar to that described in the FBI report to launch attacks on businesses in highly destructive attacks in South Korea and the Middle East, including one against oil producer Saudi Aramco that knocked out some 30,000 computers. Those attacks are widely believed to have been launched by hackers working on behalf of the governments of North Korea and Iran.

Security experts said that repairing the computers requires technicians to manually either replace the hard drives on each computer, or re-image them, a time-consuming and expensive process.

Monday’s FBI report said the attackers were "unknown."

Yet the technology news site Re/code reported that Sony was investigating to determine whether hackers working on behalf of North Korea were responsible for the attack as retribution for the company’s backing of the film "The Interview."

The movie, which is due to be released in the United States and Canada on Dec. 25, is a comedy about two journalists recruited by the CIA to assassinate North Korean leader Kim Jong Un. The Pyongyang government denounced the film as "undisguised sponsoring of terrorism, as well as an act of war" in a letter to U.N. Secretary-General Ban Ki-moon in June.

The technical section of the FBI report said some of the software used by the hackers had been compiled in Korean, but it did not discuss any possible connection to North Korea.

Manual Account Hijacking Is Lucrative Exploit for Digital Bad Guys

A vast majority of research focuses on automated and/or botnet exploits, which makes sense when considering the number of victims affected. However, a research team from Google and the University of California, San Diego chose a different path, looking at "manual account hacking." Exploits that are rare - less than nine incidents for every one million people who use Google daily. "However, the damage manual hijackers incur is far more severe and distressing to users and can result in

significant financial loss," the researchers mention in their paper Handcrafted fraud and extortion: Manual account hijacking in the wild. "These needle-in-a-haystack attacks are very challenging and represent an ongoing threat to internet users."

To start, there are two types of account hijacks:

* Automated account hijacking: Attacks that try to compromise user accounts via botnets or spam networks. This attack uses automated tools, attempting to maximize the attacker’s ROI by scamming a small amount of money from thousands of victims.

* Manual account hijacking: The bad guys hijack accounts looking for ways to steal money, ransom applications or data, leverage contact information for future attacks, or use sensitive personal data against the victim.

To explain the difference between automated exploits and manual attacks, the paper mentions, "Manual hijackers spend significant non-automated effort on profiling victims and maximizing the profit - or damage - they can extract from a single credential."

The graph to the right depicts the relationship between number of accounts hijacked and the "depth of exploitation." It seems we can be thankful the more prevalent automated exploits are less exploitative.

The first step is stealing a victim’s account login information. The paper mentions the most sought-after account is email followed by online financial accounts. For this discussion, the focus will be limited to email-account hijacking.

Once attackers have the login information, they decide quickly whether the account is worth further effort. The paper explains, "If the brief account value exploration yields promising results, the hijackers spend an additional 15 to 20 minutes per account sifting through emails, and finding ways to monetize the account."

The hijackers are hoping to find emails holding financial or personal data they can use on the current victim or improve their chances of exploiting the victim’s contacts by making the scam email supposedly from the victim seem more realistic.

The profiling portion of the attack was of special interest to the researchers. They mention, "This systematic assessment phase and the fact that certain accounts are not exploited suggest that manual hijackers are ’professional’ and follow a well-established playbook designed to maximize profits."

The researchers offer more evidence that well-organized groups are behind manual account hijacks:

* The individuals seemed to work according to a tight daily schedule. They started around the same time every day, and had a synchronized, one-hour lunch break. They were inactive over the weekends.

* All individuals followed the same daily time table, defining when to process the gathered password lists, and how to divide time between ongoing scams and new victims.

* They were operating from different IPs, on different victims, and in parallel with each other, but the tools and utilities they used were the

same. They also shared certain resources such as phone numbers.

More validation for experts who contend online-crime syndicates are run with business-like precision.

Most individuals, at one time or another, have received an email where someone is in trouble and needs money. Almost at once the scam is dismissed because the email - an automated account hijacking attempt - makes little sense. However, manual account hijacks are different. Being non-automated, attackers can inject material to personalizing the scam email.

The research team mentions there is a distinct pattern to most of the scam emails. They all tend to have:

* A story with credible details to limit the victim suspicion.
* Words or phrases that evoke sympathy and aim to persuade.
* An appearance of limited financial risk for the plea recipient as financial requests are requests for a loan with concrete promises of speedy repayment.
* Language that discourages the plea recipient from trying to verify the story by contacting the victim through another means of communication, often through claims that the victim’s phone was stolen.

* An untraceable, fast, and hard-to-revoke yet safe-looking money transfer mechanism.

The research paper then describes what email providers can do to prevent manual account hacking. Sadly, there are precious few for-sure user defenses other than second-factor authentication - if it is available use it. Two-factor authentication will thwart the bad guys.

All PayPal Accounts Were 1 Click Away from Hijacking

Until Egyptian cyber-security researcher Yasser Ali found it and reported it to PayPal, there was a security hole that meant 150 million-plus customers were one measly click away from account hijacking.

Ali said in a blog post that the "critical vulnerability" meant an attacker could hijack any PayPal user account and have their way with it, including but not limited to the ability to:

Add/remove/confirm email address
Add fully privileged users to a business account
Change security questions
Change billing/shipping address
Change payment methods
Change user settings (notifications/mobile settings)

In other words, an attacker could have picked an account, exploited the hole, and gone on to install their own contact details and to switch the billing, shipping address and payment methods as they liked.

Ali also showed how it’s done in this proof of concept video.

The researcher said that the exploit was enabled by a cross-site request forgery (CSRF) - also known as a "session riding" - flaw. Such an exploit

provides a way for malicious website X to retrieve data that is only supposed to be revealed when you visit site Y.

All it would have taken, he said, was to convince a target to click a link, which is simple enough with a little help from social engineering: for example, by sending a link via email or chat.

Ali's now $10,000 (£6,380) richer, having bagged the top payout in PayPal's bug bounty program.

He said in his advisory that the captured authentication token his exploit managed to obtain was valid for all PayPal accounts.

After a deep investigation I found out that the CSRF auth is reusable for a specific user email address or username.

This means attackers who found any of these CSRF tokens can [imitate] any logged in user.

[Attackers] can obtain the CSRF auth by intercepting the POST request from a page that provides an auth token before the logging-in process.

PayPal confirmed the bug to Vulture South - also known as The Register's Asia-Pacific bureau.

A spokesperson said that the company hasn't detected any evidence of accounts having been compromised.

From the statement:

Through the PayPal Bug Bounty Program, one of our security researchers recently made us aware of a way to bypass PayPal's Cross-Site Request Forgery (CSRF) Protection Authorization System when logging onto PayPal.com. Our team worked quickly to address this vulnerability, and we have already fixed the issue.

CSRF isn't a new kind of exploit, it just doesn't seem to get the same attention that SQL injection or XSS (Cross Site Scripting) do.

If you build websites for people we recommend you read the OWASP has guides on how to review code for this particular vulnerability, how to test for it, how to prevent it, and more.

You can defend yourself against CSRF vulnerabilities when you're browsing or reading your mail just by making sure you log out of websites and applications when you're finished with them.

Beware The Santa Claus Letter Scam

No, Virginia, there is no Santa Claus. At the very least, Saint Nick is not offering to send you or your loved ones a special holiday greeting via email.

Editors at Yahoo Tech have received more than a dozen spam emails promoting Letters from Santa, a chestnut of scam that is almost as old as the Internet itself. They generally ACT like this:

Clicking the Check It Out Now! link inside each of these messages brings you to the Official Letters From Santa 2014 site, where for the low, low price of just $19.95 you can ask the jolly old fella to send an official Christmas greeting to your wee ones.

We don t recommend it. At the very minimum, you re paying $20 for a piece of paper. More likely, you won t get anything at all for your money. Worse, these clowns now have your name, email address, and credit card information.

Here s one way to tell it s a scam: Look at the badges on the bottom of the shopping cart professing how secure, reliable, and trusted the site is.

If these badges were genuine, you d be able to click each one and be taken to a site that verifies its authenticity. Click on these, however, and nothing happens. They re just static images. Scam, hello?

This is hardly the only site operated by these jokers. They also run Santa s Official Naughty List, where you can allegedly have Santa send You ve Been Naughty grams to your loved ones. The same outfit is behind Magical Christmas Packages, Santa s Angry, Santa s Not Happy, North Pole Magic Snow, and others.

The contact address for the site links to a variety of Florida-based companies (or one company with many names), including Prime Time Ads Inc., Attractive Ads Media, Multi-Meridian Inc., Connectivity Marketing and Media, and Premium Source Nutrition.

Calling the toll-free number listed on the Santa websites produces nothing but silence. Calls to an anonymous voice mailbox at Attractive Ads Media, listed on the Naughty List domain registration, were not returned.

What else do these people sell? Well, fake facelifts in a bottle, for one. Ever wonder how Santa maintains his youthful appearance, despite being, like, a thousand years old? Now you know.

More likely, though, is that these emails came not from the North Pole or Florida but from Russia. Domains used to redirect links inside the faux Santa emails are registered to email addresses and phone numbers in the former Soviet Union.

There may well be legitimate sites that promise to send your kids a letter from Santa, but these aren t it.

Airport Busts for 118 Credit Card Fraudsters

A global operation to tackle online fraud led to 118 arrests across 80 airports last week, Europol has revealed.

The European police agency announced on Friday how its ’Global Airport Action’ had targeted criminals who bought plane tickets online with fake or stolen credit card details.

The operation, coordinated by Europol s Cyber Crime Centre (EC3), brought together over 80 airports, more than 60 airlines, a large number of banks

and law enforcement agencies in 45 countries, as well as representatives from the major credit card companies.

Europol, along with Interpol and Ameripol, flagged up a total of 281 suspicious transactions as part of its operation to tackle fraudulent online ticket booking, a crime it says costs the airline industry $1bn (£639m) per year.

The agency said that many of those arrested in the latest operation were repeat offenders who had been previously arrested at airports.

Europol Director Rob Wainwright hailed the operation as a success:

This operation is another example of law enforcement and the private sector working seamlessly together, to prevent and fight cybercrime - this time identity theft and credit card fraud. We are reaching new levels with our cooperation and aim to become an ’unbeatable alliance’ with aspirations to make cyberspace as crime free as possible for global citizens.

It’s also good news for consumers, especially in the wake of high profile breaches such as that of Home Depot which left 56 million unique payment cards exposed.

The announcement comes in the same week that investigative reporter Brian Krebs revealed how credit card fraudsters have got into the Thanksgiving spirit by offering Black Friday and Cyber Monday deals on credit and debit card ’dumps’, swapping large swathes of payment card data for as little as $100.

German Court Blocks US Extradition for "Number Two" Hacker

A German court has put the brakes on efforts to extradite a suspected hacker to the US, arguing that the potential sentence of almost 250 years he faces there is excessive by German standards.

32-year-old Turkish national Ercan Findikoglu has been held in Germany since his arrest at Frankfurt Airport in December 2013. Since then there have been several legal stages, with approval given to the extradition by a regional court in August of this year.

Now the country’s highest court, the Federal Constitutional Court of Germany or Bundesverfassungsgericht based in Karlsruhe, has overturned that decision, questioning both the extreme length of the sentence threatened by US authorities, and also the inclusion of a "conspiracy" charge not compatible with German law.

The decision was made on November 20th, and details were revealed this week by news magazine Der Spiegel, which played a major part in revealing the NSA secrets leaked by Edward Snowden.

Earlier Spiegel Online reports (in German) connect Findikoglu to massive global card heists in late 2012 and early 2013, involving hacking of systems in India operated by payment processing firms EnStage and ElectraCard.

In lengthy penetrations the hackers were able to doctor accounts for

prepaid debit cards, removing withdrawal limits so that a team of carders armed with stolen PINs and cloned cards could take out large sums in orchestrated cash-outs.

In separate swoops targeting the two companies, it’s believed at least $45 million was withdrawn from ATMs around the world, including over 140 in New York alone.

The first heist, involving cards from the National Bank of Ras Al-Khaima (RAKBANK), UAE, stolen in the ElectraCard hack, seems like something of a practice run, scoring a mere $5 million in December 2012.

The second targeted the Bank of Muscat, Oman, via its partner EnStage and scooped an epic $40 million, with 36,000 ATM transactions carried out in the space of 10 hours in February of last year.

Several of the low-level carders and cashers have already been brought to justice, including a crew in New York, and more recently a German mother-and-son team given over four years for nabbing 168,000 Euros from ATMs in Dusseldorf.

Now it looks like one of the ringleaders is making his slow way through the international justice system, complicated as ever by the complexities of international law.

It’s not the first time the US preference for extreme potential sentences, usually used as leverage to assure easy guilty pleas, have caused a snag in cybercrime extradition proceedings. Last year similar complaints of excessive sentencing held up the extradition from Latvia of a man suspected of being behind the Gozi Trojan.

In that case the matter was swiftly resolved, and it seems likely that this one will eventually go the same way, with a little flexibility and understanding on both sides.

Further complicating matters is a second extradition request from Turkey for Findikoglu, again according to Der Spiegel.

Findikoglu also has form in these struggles, with reports dating back to 2008 of involvement with a series of cyber thefts including a failed heist targeting over a million stolen card numbers.

He was described at the time as "the world’s number two hacker", and was even then facing a possible 200 year sentence in the US but may have only served a couple of years in Turkey.

In this case, should he eventually make his way to the US, he’s likely to get a rather more serious sentence.

It should of course be appropriate for the scale of his crimes, but surely most people would agree that even for a repeat offender, more than three full lifetimes may be a little harsh.

Indicted Internet Entrepreneur Dotcom Avoids Jail

Indicted Internet entrepreneur Kim Dotcom on Monday defeated efforts by prosecutors to send him back to a New Zealand jail or make him wear an

electronic monitoring bracelet but says his long-running legal battle has left him broke.

After a three-day hearing, Auckland District Court Judge Nevin Dawson ruled there was no evidence Dotcom had secret assets or posed a flight risk, according to Fairfax Media.

U.S. and New Zealand prosecutors had sought to have Dotcom's bail revoked, arguing he might try to flee the country after earning tens of millions of dollars since his 2012 arrest. Prosecutors said he'd breached his bail conditions in several ways, including indirectly contacting a former associate.

Dawson did tighten Dotcom's bail conditions by ruling he can no longer travel by private helicopter or boat and must report to police twice a week, Fairfax reported. But the judge said it would be inappropriate to deprive Dotcom of his freedom on the evidence presented.

The German-born Dotcom is fighting attempts by U.S. prosecutors to extradite him on racketeering charges over his website Megaupload, which authorities shut down at the time of his arrest. His extradition hearing has been delayed several times and is now scheduled for June.

Prosecutors say Megaupload was used to illegally download millions of songs and movies in one of the biggest copyright cases in history. But Dotcom says he can't be held responsible for those who chose to use Megaupload for illegal downloads.

At the time of his arrest, authorities froze Dotcom's worldwide assets, which were worth over $40 million, and jailed him for a month.

But since then, Dotcom says he has earned another 40 million New Zealand dollars ($31 million) from new ventures, including the file-sharing site Mega and a music venture, Baboom.

But he also spent several million dollars on a failed political campaign and says his legal case has so far cost him more than NZ$10 million.

He told the unBound Digital conference by video link last week that he was "officially broke," which had caused his New Zealand lawyers to abandon him after working for more than two years on his case. He blamed prosecutors for his predicament.

"They have certainly managed to drain my resources, and dehydrate me, and without lawyers I'm defenseless," he told the conference.

He later clarified on Twitter that he'd paid the rent on the mansion he lives in near Auckland through mid-2015 and that he would return to court soon, seeking to have some of his frozen assets released to pay his legal fees and living expenses.

Supreme Court To Consider Facebook Threats Case

The Supreme Court is weighing the free-speech rights of people who use violent or threatening language on Facebook and other social media.

The justices will hear arguments Monday in the case of a man who was

sentenced to nearly four years in prison for posting graphically violent rap lyrics on Facebook about killing his estranged wife, shooting up a kindergarten class and attacking an FBI agent.

Anthony Elonis of Bethlehem, Pennsylvania, says he was just venting his anger over a broken marriage and never meant to threaten anyone.

But his wife didn't see it that way, and neither did federal prosecutors. A jury convicted Elonis of violating a federal law that makes it a crime to threaten another person. A federal appeals court rejected his claim that his comments were protected by the First Amendment.

Lawyers for Elonis argue that the government must prove he actually intended his comments to threaten others. The government says it doesn't matter what Elonis intended; the true test of a threat is whether his words make a reasonable person feel threatened.

One post about his wife said, "There's one way to love you but a thousand ways to kill you. I'm not going to rest until your body is a mess, soaked in blood and dying from all the little cuts."

The case has drawn widespread attention from free-speech advocates who say comments on Facebook, Twitter and other social media can be hasty, impulsive and easily misinterpreted. They point out that a message on Facebook intended for a small group could be taken out of context when viewed by a wider audience.

"A statute that proscribes speech without regard to the speaker's intended meaning runs the risk of punishing protected First Amendment expression simply because it is crudely or zealously expressed," said a brief from the American Civil Liberties Union and other groups.

So far, most lower courts have rejected that view, ruling that a "true threat" depends on how an objective person perceives the message.

For more than four decades, the Supreme Court has said that "true threats" to harm another person are not protected speech under the First Amendment. But the court has been careful to distinguish threats from protected speech such as "political hyperbole" or "unpleasantly sharp attacks."

Elonis argues that his online posts under the pseudonym "Tone Dougie" were simply a crude and spontaneous form of expression that should not be considered threatening if he didn't really mean it. His lawyers say the posts were heavily influenced by rap star Eminem, who has also fantasized in songs about killing his ex-wife.

But Elonis' wife testified that the comments made her fear for her life. After his wife obtained a protective order against him, Elonis wrote a lengthy post mocking court proceedings: "Did you know that it's illegal for me to say I want to kill my wife?"

A female FBI agent later visited Elonis at home to ask him about the postings. Elonis took to Facebook again: "Little agent lady stood so close, took all the strength I had not to turn the bitch ghost. Pull my knife, flick my wrist and slit her throat."

The Obama administration says requiring proof that a speaker intended to be threatening would undermine the law's protective purpose. In its brief to the court, the Justice Department argues that no matter what someone

believes about his comments, it doesn’t lessen the fear and anxiety they might cause for other people.

The case is Elonis v. United States, 13-983.

Man Jailed After Posting Ex’s Topless Photos to Her Employer’s Facebook Page

A US man from Los Angeles who hid behind a pseudonym to post topless photos of his ex to her employer’s Facebook page has been found guilty and jailed.

His ex-girlfriend had taken out a restraining order in November 2011 after the man sent harassing text messages following the breakup of their four-year relationship.

Noe Iniguez, 36, broke that restraining order to jump online, use an alias, and call the woman "drunk" and a "slut" in his posts as he urged the company to fire her.

Iniguez thus becomes the first person to be convicted under a revenge porn law that California passed in October 2013.

Los Angeles City Attorney Mike Feuer on Monday said that Iniguez was convicted on three criminal counts, including two restraining order violations and the state revenge porn statute, following a seven-day jury trial.

Iniguez was sentenced to one year in jail and three years of probation, ordered to attend domestic violence counseling, and ordered to stay away from his victim.

California’s revenge porn statute prohibits the unauthorized posting of nude or sexual images of an individual with the purpose of causing emotional distress.
Since 2013, 13 states have passed similar legislation.

In 2014, bills were introduced or are now pending in at least 28 states, the District of Columbia and Puerto Rico, according to the National Conference of State Legislatures.

England and Wales also now have a revenge porn law.

In mid-November, an ex-boyfriend who swapped out his WhatsApp profile picture for a naked picture of his ex-girlfriend was thought to be the first person in England to be jailed for the offence.

Feuer said that Iniguez’s conviction should show that California’s new law has teeth:

California’s new revenge porn law gives prosecutors a valuable tool to protect victims whose lives and reputations have been upended by a person they once trusted. This conviction sends a strong message that this type of malicious behavior will not be tolerated.

California’s law, with its requirement that prosecutors prove that accused people intended to cause emotional distress, is a more narrowly focused law than some others out there.

Arizona in particular went for a broader sweep when it tried to ban all posts showing anyone "in a state of nudity or engaged in specific sexual activities" unless the person pictured had given their explicit permission.

A coalition of free-speech advocates protested, claiming that the existing laws were thrown together so shabbily, they could arguably be used to criminalize a host of non-vengeful innocents who handle nude images: libraries, booksellers, college professors, breastfeeding educators, or news outlets.

Arizona wasn’t the only state to take such a broad approach to revenge porn legislation, but it was seen as likely the worst, given that it didn’t limit itself to criminalizing malicious disclosures, according to Michael Bamberger, one of the ACLU’s attorneys on the case:

This is probably the most egregious, because it has no requirement for malicious intent and no exception for images that are newsworthy. It applies to republication by people who have no idea how the image was first obtained.

A judge subsequently halted enforcement of Arizona’s law pending a rewrite.

According to the BBC, the Scottish government is also considering enacting its own revenge porn law, and there are calls in Ireland for the same.

It’s good to see prosecutors armed with well-written laws to protect those who suffer from belligerent acts of revenge porn.

Hopefully, the states and countries that have yet to enact legislation will take a page from the Arizona free-speech fracas and craft their legislation with an eye to protecting those who post nude images without the intention of causing emotional distress.

Of course, "emotional distress" doesn’t cover the gamut of suffering revenge porn victims experience as their tormentors seek to trash their victims’ reputations, poison their ability to get or remain employed, or even threaten their physical safety.

But it’s a good enough term to serve as shorthand for those many forms of suffering.

It’s wise to make sure that the notion of intent is included in legislation, lest we end up with lousy laws that trample on free speech and which could be used to persecute those who post nude photos without a scrap of malice in their hearts.

Newest Preview of Windows 10 Reportedly Coming Next Month

Windows 8 has been a massive disappointment for both Microsoft and for PC owners around the world. But it looks like we re getting closer to the next edition of the company s operating system.

According to The Verge, Microsoft will show off the consumer version of

its upcoming Windows 10 during an event scheduled for late January.

The event will reportedly focus on the consumer enhancements included in Windows 10. The company will also discuss how Windows 10 will serve as a single platform for Windows-based PCs, tablets, phones, and the Xbox One.

Microsoft has yet to confirm a release date, but Windows 10 should be available sometime in 2015.

Microsoft previously showed off an early version of Windows 10 during an event in September, but primarily focused on how business users stand to benefit from the operating system.

Still, what we saw from Windows 10 gave us some hope. The biggest improvement to the operating system is that the Start button is making its triumphant return. The new Start button gets a slick new look that appears to be a combination of the classic Windows start menu and Windows 8 s tile interface.

Desktop and laptop users will also be happy to learn that the classic Windows Desktop is back. The tile interface can still be accessed on the PC version of Windows 10, but it will take a backseat to the desktop screen.

What s more, Windows 8-style apps will now be accessible from the desktop, something you couldn t do with Windows 8. Oh, and you ll now be able to snap both desktop programs and Windows apps on either side of the screen at the same time. Previously, you could snap only Windows apps.

Microsoft isn t giving up on 2-in-1 devices with Windows 10. The company s new Continuum mode will focus on the operating system s desktop mode when using your device as a laptop but switch over to the more touch-friendly tile interface when using it as a tablet.

We haven t heard much about what the consumer preview of Windows 10 will offer, but based on what we ve already seen from the operating system, Windows 10 may be a return to form for Microsoft.

First Pictures, Video of Cortana Running in Windows 10 Surface

Microsoft s answer to Siri and Google Now surfaced earlier this year as Cortana. The virtual assistant is already available on Windows Phone devices and is all but guaranteed to show up in Windows 10 we just haven t see any hard evident of it yet that is, until now.

WinBeta managed to get access to a version of Windows 10 with Cortana. It s worth pointing out that this is an early, pre-release version meaning the final product will look much more polished than it does in the clip below.

The Cortana experience in Windows 10 will pretty much mirror what s already available on mobile. For example, users will be able to search maps and get traffic information, set reminders, call people via Skype, control music playback and check the weather, among other things.

As you can see, Cortana doesn t yet have a personality in this early build so you can t ask it personal questions like Who are you? and so

forth. This functionality is expected to come baked into the final consumer version, however.

One unknown at this hour is whether or not Windows 10 users will be able to activate Cortana hands-free. Such ability would of course be convenient but we ll have to wait to see what Microsoft has in store next year.

Microsoft launched a Technical Preview of Windows 10 a few months ago for enthusiasts to check out. A consumer-friendly preview of the OS is expected in early 2015 followed by the actual product launch in late summer or early fall.

Firefox 34 Makes It Official: Google Is Out, Yahoo Is In

Firefox 34, which includes eight security fixes, is the first version since Mozilla announced it was dropping Google for Yahoo as its default search engine.

Firefox 34 is now out, and with it, users gain new search and communication features as well as fixes for eight security issues.

The latest release of Mozilla’s open-source Web browser is particularly noteworthy in that it is the first Firefox release since Mozilla’s announcement on Nov. 19 that it was ending its decadelong search partnership with Google.

In Firefox 34, Yahoo is now the default search provider for users in the United States, while Yandex is now the default in Russia and Baidu is the default in China. The search bar itself has also been improved to more easily enable users to use different search engines beyond just the default search provider, meaning that while Yahoo is now the default search engine for those in the U.S., users can easily change the default back to Google.

Mozilla is also introducing its Firefox Hello WebRTC (Web Real Time Communications) feature in the stable release of Firefox 34. The promise of Firefox Hello is that users will be able to easily make voice calls using only the browser. Chad Weiner, director of product management for Firefox at Mozilla, explained to eWEEK that even though the Firefox Hello feature is in the stable, generally available Firefox 34 release, it will still have a beta label.

"We don’t do this often, but sometimes we iterate so much on a feature in its formative stages, even when it is available to our release channel, that it makes more sense to still designate a feature as being in a beta state, even as it is available to a mass audience," Weiner said. "We’re confident in the performance of the feature, but it’s still new so we expect to have to work out some bugs along the way."

In terms of what’s next, Mozilla is looking at ways to bring collaboration elements to Hello so users can share more online experiences and be more productive, he said.

From a security standpoint, Firefox 34 is the first Firefox release to completely disable support for the Secure Sockets Layer (SSL) 3.0 cryptographic protocol. SSL 3.0 was revealed to be at risk of exploitation

from the POODLE vulnerability. Rival browser vendor Google, meanwhile, decided to initially only drop fallback compatibility for SSL 3.0 with the Chrome 39 browser and is not expected to drop SSL 3.0 support entirely until Chrome 40 later this month.

"Dropping support for SSLv3 entirely protects more users from its inherent vulnerabilities," Weiner said. "We're putting users' safety online first and trying to aggressively push the Web toward more secure alternatives."

As part of the Firefox 34 release, Mozilla has issued eight security advisories, three of which are rated as being critical.

Among the critical advisories is one that most Firefox releases include for what Mozilla refers to as "Miscellaneous memory safety hazards." The second critical advisory is for a use-after-free memory issue in HTML5 parsing that is identified as CVE-2014-1592.

The third critical security advisory is for a buffer overflow issue identified as CVE-2014-1593, which was reported to Mozilla by a Google security researcher.

"Security researcher Abhishek Arya (Inferno) of the Google Chrome Security Team used the Address Sanitizer tool to discover a buffer overflow during the parsing of media content," Mozilla's security advisory warns. "This leads to a potentially exploitable crash."

The Address Sanitizer tool is open-source technology from Google that is used by security researchers to help identify potential use-after-free flaws in software code.

I Am Not A Robot: Google Swaps Text CAPTCHAs for Quivery Mouse Clicks

Remember back in 2013, when Ticketmaster - the world's largest online ticket retailer - decided to stop torturing people's eyeballs by making them decipher blobs of melted characters in order to prove that they're human?

Likewise, Google's now too stabbing a fork into CAPTCHA, the aggravating test that's supposed to determine if we're robots or scripts used by spammers or other online misdeed-doers, or if we are instead real, live, warm-blooded simians.

CAPTCHA came out of Carnegie Mellon University and stands for "Completely Automated Public Turing test to tell Computers and Humans Apart".

The tests are designed to be hard for robots, easy for humans.

They typically consist of typing letters and/or digits from a distorted image.

Or, as the case may be, messages to go pleasure yourself. Or, then again, mathematical problems that make your brain bleed.

Ten years into using CAPTCHA to keep robots from engaging in dirty tricks online, the "supposed to weed out bots" has now turned into "utterly stink at weeding out bots".

That’s because advances in Artificial Intelligence have resulted in robot creations that are now able to solve even the most difficult variant of distorted text with 99.8% accuracy, according to Google’s recent research.

Not that Google’s going to stop testing site visitors to weed out bots, mind you.
Rather, as it announced on Wednesday, Google’s going to move away from asking users to read blobby text and type it into a box, as it’s been doing, like this:

And instead will simply ask us, "Are you a robot?" with what it’s calling the "No CAPTCHA reCAPTCHA" API, like so:

Asking us to check off a box saying that "I am not a robot" will be an effective way of determining whether or not we’re robots because humans move their cursors in a humanlike way.

Specifically, the difference between bot and human can be revealed in clues as subtle as how a user (or a bot) moves a mouse in the brief moments before clicking the "I am not a robot" button, according to Vinay Shet, the product manager for Google’s Captcha team.

Without realizing it, humans also drop clues that can establish whether we’re automated or not: IP addresses and cookies show our movements elsewhere on the Web and can help prove that we’re not a bad actor.

Wired quotes Shet:

All of this gives us a model of how a human behaves It’s a whole bag of cues that make this hard to spoof for a bot.

He said that there are other variables that will help make the determination, but those have to be kept secret, lest botmasters figure out how to work around them and once again learn how to slip past Google’s filters.

Google’s been integrating automated bot-detection into its CAPTCHAs since at least 2013.

In October 2013, Google revealed that it had developed what it called its Advanced Risk Analysis backend for reCAPTCHA to filter out bots.

The backend doesn’t just look at whatever gobbledygook we type into the box. Rather, it observes our entire engagement with a CAPTCHA, from start to finish - before, during, and after we type into the box - to determine whether we’re carbon-based.

On Valentine’s Day, Google gave us a taste of what reCAPTCHA can do, presenting us with chocolates and flowers and throbbing hearts - the first two of which were rendered in text that was simple (for humans) to read.

It sounds great, but it’s not yet time to kiss the inscrutably distorted CAPTCHA blobs goodbye.

Over the past week, Google’s tests on sites that use CAPTCHA have verified most humans, but it still missed quite a few. As Wired reports, about 60% of WordPress users and 80% of users at video game sales site Humble Bundle got past the CAPTCHA with only the simple checkbox.

When Google’s Advanced Risk Analysis engine can’t figure out what we are with a mere click, it’s going to back up the test with a pop-up window that will present users with the same old distorted text we’ve been enduring for years.

For mobile users, things haven’t gotten quite so simple as a single click. But when they face a CAPTCHA on their mobile phone or tablet, they’ll now have a much easier hurdle to leap: rather than having to type in text, they’ll be asked to select all the images that correspond with a clue image.

Like Google says, it’s a lot easier to tap photos of cats or turkeys than to type in a line of text on a phone:

And if you’re worried about the privacy implications of Google analyzing where your mouse moves on a page, Shet pointed out that Google will only be tracking your movements over the CAPTCHA widget when it appears on other sites, not on the entire page.

This is how he put it to Wired:

You don t have to verify your identity to verify your humanity.

Besides, as we’ve noted before, tracking movement is not just a Google thing.

Facebook, Twitter, Gmail or any webpage can track everything you do and could be keylogging your every pointer movement or keystroke.

Logging keystrokes is no super secret, privacy-sucking vampire sauce. It’s plain old Web 1.0. This is not news, but it’s certainly worth repeating: anybody with a website can capture what you type, as you type it, if they want to.

The reality is that JavaScript, the language that makes this kind of monitoring possible, is both powerful and ubiquitous.

It’s a fully featured programming language that can be embedded in web pages, and all browsers support it. It’s been around almost since the beginning of the web, and the web would be hurting without it, given the things it makes happen.

Among the many features of the language are the abilities to track the position of your cursor, track your keystrokes and call "home" without refreshing the page or making any kind of visual display.

Those aren’t intrinsically bad things. In fact, they’re enormously useful. Without those sort of capabilities sites like Facebook and Gmail would be almost unusable, searches wouldn’t auto-suggest and Google Docs wouldn’t save our bacon in the background.

In the case of Google’s advances with reCAPTCHA, such an ability can stop a lot of bad bots from doing things that can be worse than the annoyance of having to endure typing in text from a blobby image.

Think bots that harvest email addresses from contact or guestbook pages, site scrapers that grab the content of websites and re-use it without permission on automatically generated doorway pages, bots that take part in Distributed Denial of Service (DDoS) attacks, and more.

I’ll take the kittens, please!

Microsoft Is Killing Off Clip Art for Word and PowerPoint

Back in the 90s, Clip Art took over Word and PowerPoint files thanks to the thousands of office workers and students who used the images as a way to improve their documents. These days there are a large number of free images available on the web, and Microsoft is recognizing this by killing off its Clip Art portal in recent versions Word, PowerPoint, and Outlook. The Office.com Clip Art and image library has closed shop, explains Microsoft s Doug Thomas. Usage of Office s image library has been declining year-to-year as customers rely more on search engines.

While most references to Clip Art disappeared with Office 2013, users were able to insert the old-school images into documents using an Office.com Clip Art option. That is now being replaced by Bing Images, with Microsoft filtering images to ensure they re based on the Creative Commons licensing system for personal or commercial use. Most of the new images are much more modern, instead of the illustrated remnants of the past. Clip Art might be facing the same Office-related demise as the great Clippy assistant.

Apple Co-Founder Steve Wozniak Says It s a Bit of a Myth The Company Started in a Garage

If you didn t start your company in a garage, it can t be much of a company, can it?

After all, a fine modern company needs a legend of bootstrapped pain, dripping roofs, and hordes of chilly engineers huddled in a place only big enough for a Honda Legend.

Sometimes, though, that s what these stories are: legends.

For decades, many thought that Apple s formative years were spent with a whiff of gasoline hanging in the air. Yes, it all happened in the garage of Steve Jobs childhood home in Los Altos, Calif. Or did it? In an interview with Bloomberg, Apple co-founder Steve Wozniak poured cold water on the story.

He said: The garage is a bit of a myth. It s overblown. The garage represents us better than anything else, but we did no designs there. We would drive the finished products to the garage, make them work, and then we d drive them down to the store that paid us cash.

Woz explained that the fledgling Apple outgrew that garage very quickly.

He added: There were hardly ever more than two people in the garage and mostly they were sitting around kind of doing nothing productive.

Well, yes. But it s a great story, isn t it? Once you re a success, tossing your company s history into a field of magical distortion makes it all sound a little more romantic than it probably was.

We don t need people and companies to be successful. We also want their stories to be moving, inspiring and, most of all, movie-worthy.

Who wants to see a movie about a company with a good idea that buys a big factory, employs lots of people and pleases even more? How dull.

Ten Terrible Tech Annoyances That Should Be Illegal

Today s technology is astonishing, magical, and delightful. It can also be annoying beyond belief. How many times have you yelled, There oughta be a law! at a product or website, wondering who in their right mind could have released a certain feature into the world?

And you re right. There oughta.

Someday, the editors of Yahoo Tech will rule the world. And we will work swiftly to enact laws that fix the most annoying things in technology:

1. CAPTCHAs shall be banned

CAPTCHAs are these dumb things:

They are readability roadblocks on websites. They re supposed to prevent automated spammer software from signing up for fake accounts, but it s a losing game. Computers are getting smarter all the time. Humans are not. In order to make CAPTCHAs too hard for computers to read, they ve had to become too hard for humans to decipher. It s time for them to go.

2. Hold music and the right of silence?If you have to wait on the phone to talk to a person or a machine, why should you be subjected to awful music? We decree that there shall be an option for silence, maybe with a periodic, quiet update that you re still on hold. You know, so that you can actually focus on something else instead of having some horrible din blasting in your ear.

3. Proprietary power bricks: Illegal?We now have several devices per person, and it s nearly impossible to keep them all paired up with the power adapters they came with.

From now on, all small electronic gizmos shall be powered by USB cables, so you can charge them either from your computer or with a ubiquitous USB power plug adaptor.

In fact, in Europe, there s already a common charger law. Progress! Let s bring that law to the United States and extend it to all small electronics, not just mobiles.

(By the way, it s too bad Apple s Lightning connector is proprietary, since it provides a better user experience than micro USB, but perhaps when USB Type C comes out, Lightning will finally have a worthwhile competitor.)

4. Printer ink to get consumer advisory labels?The most expensive liquid you can buy is not gasoline, champagne, or even fancy perfume. It s inkjet printer ink, packaged into a little disposable printhead. It works out to about $8,000 a gallon.

Those absurd prices drive the retail costs of printers down to the toy category. But people should know what they re in for. From now on, printer advertisements shall include estimated yearly ink cartridge costs, just as refrigerator labels come with yearly energy costs. And printer ink cartridges shall be sold on a dollars-per-ounce basis, so we re all aware of what we re spending money on.
Watch: What s Inside an Inkjet Cartridge?

5. No voice-response double jeopardy

An automated telephone system asks you to enter your name, account number, or other information. OK, fine. Then why, once we re transferred to a human operator, must we be asked for the same information again?

It won t happen in the Yahoo Tech future. That practice will be outlawed
6. Alerts must know their place?Our sanity is more important than a random notification or alert from our technology. Monitor status messages shall be designed so they don t block login windows. Appliances like microwaves and dishwashers shall not beep constantly about minor issues, like their cycles being done (once or twice is enough), or their doors being closed.

I want to log in to my computer, not get some unnecessary information about the monitor s refresh rate.

7. Non-removable batteries: Banned?A technology product can last nearly indefinitely, but a chemical battery (at least today) has a limited lifespan. Once you start using a product with a lithium-ion battery, it starts to degrade. To keep the product from becoming obsolete before you re done with it, batteries shall be easily replaceable.

We are not tyrants, though. We will not decree that all batteries must be under cheeseball snap-on covers. Just that a normal human, with a standard tool (maybe a jeweler s screwdriver), will be able to replace a device s batteries without requiring a technical degree or a trip to an Apple Store.

8. Software updates shall only update?When a software product tries to update itself, it shall do that and only that. An update process shall not be used to download and install a third-party app. We ll call this the Don t Ask law, after the Ask toolbar ride-along install that often comes along with Java or Adobe Flash updates.

9. Pasted text must default to no formatting ?If you copy text from a website and want to paste it into an email or another document, you get mismatched formatting. Like this:

Henceforth, pasted text shall inherit the formatting of the document into which it is being pasted, unless the paster holds down some special option key to override that behavior. The way copy/paste works now is the reverse of common sense.

10. No more long ads before video content?The maximum length of a pre-roll ad (the commercial that plays before a video online) shall be at most 15 percent the length of the video itself. No more 30-second advertisements in front of 17-second videos.

Advertising makes free videos possible, of course, so we won t decree it out of existence. But keeping the ad-to-content ratio reasonable should keep readers and viewers more engaged, and as a byproduct lead to

snappier ads.

And while we re at it, we might also ban auto-play videos (video streams that start up immediately when you click a webpage). Like the one on this page itself. Come visit us in jail.

=~=~=~=